UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,025	03/26/2004	John J. Apostolopoulos	200401716-1	8407

22879 7590 03/03/2009

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
HOANG, DANIEL L	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
03/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/810,025
Filing Date: March 26, 2004
Appellant(s): APOSTOLOPOULOS ET AL.

John P. Wagner, Jr., Reg. No. 35,398
For Appellant

EXAMINER'S ANSWER

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6963972	Chang	9-2000
"Recommendation for Block Cipher Modes of Operation"	Dworkin	2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chang et al., US Patent No. 6,963,972, and further in view of Recommendation of Block Cipher Modes of Operation – Methods and Techniques, hereinafter NIST.

As per claim 1, 12, 24:

Chang teaches:

A method for generating transcodable encrypted content that comprises independently processable components, said method comprising:

accessing transcodable content that comprises independently processable components to be encrypted; and

[see col. 3, lines 51-62]

encrypting at least one of said independently processable components to provide independently processable components which are independently decryptable,

[see col. 3, lines 51-62 and col. 4, lines 19-29]

said encrypting performed using an encryption scheme [that utilizes non-repeating identifiers] that uniquely correspond to said independently processable components, wherein said transcodable encrypted content is transcodable without requiring knowledge of said encryption scheme.

[see col. 10, lines 24-41]

Chang is not explicit in teaching that the encryption scheme utilizes non-repeating identifiers.

NIST teaches the Counter block cipher mode of operation (see page 15, section 6.5). The counter mode is an encryption/decryption scheme that utilizes non-repeating identifiers/counters. It would have been obvious to one of ordinary skill in the art to utilize a counter mode as the encryption algorithm used in the Chang reference. One would have been motivated to do so in order to optimize operations on a multi-processor machine where blocks can be encrypted in parallel.

As per claim 2, 13, 25, Chang teaches:

The method as recited in claim 1 wherein said independently processable components comprise components that are independently decodable and independently authenticatable.

[see col. 3, lines 51-62 and col. 4, lines 19-29]

As per claim 3, 14, 26, NIST teaches:

The method as recited in claim 1 wherein said encryption scheme comprises applying block ciphers in stream cipher mode.

[see page 15, section 6.5]

As per claim 4, 15, 27, NIST teaches:

The method as recited in claim 1 wherein said encryption scheme comprises counter (CTR) mode stream cipher encryption.

[see page 15, section 6.5]

As per claim 5, 16, 28, NIST teaches:

The method as recited in claim 1 wherein said encryption scheme comprises encrypting a counter to generate a keystream which is logically combined with plaintext to generate ciphertext.

[see page 15, section 6.5]

As per claim 6, 17, 29, NIST teaches:

The method as recited in claim 1 wherein said encryption scheme utilizes non-repeating identifiers which are non-repeating counter values.

[see page 15, section 6.5]

As per claim 7, 18, 30, NIST teaches:

The method as recited in claim 1 wherein said encryption scheme comprises performing several encryptions in parallel.

[see page 15, section 6.5]

As per claim 8, 19, 31, Chang teaches:

The method as recited in claim 1 wherein differentiating metadata that corresponds to said independently processable components is used as an input to said encryption.

[see col. 9, lines 24-45]

As per claim 9, 21, 32, Chang teaches:

The method as recited in claim 1 wherein said transcodable encrypted content has information associated with it to direct transcoding.

[see col. 10, lines 42-65]

As per claim 10, 22, 33, Chang teaches:

The method as recited in claim 1 said transcodable encrypted content comprises respective components that have respective encryption keys, wherein said respective encryption keys are related to a root encryption key.

[see col. 10, lines 24-41]

As per claim 11, 23, 34, NIST teaches:

The method as recited in claim 1 wherein said encryption scheme is selected from the group consisting of a block cipher used in output feedback (OFB) mode, RC4, SEAL, and WAKE.

[see page 13, section 6.4]

As per claim 20, Chang teaches:

The method as recited in claim 12 wherein said transcoding produces transcodable encrypted content that is smaller in size than the transcodable encrypted content that is accessed.

[see col. 9, lines 1-23]

(10) Response to Argument

I. Whether Claims 1-34 are unpatentable under 35 U.S.C. 103(a) by Chang in view of Dworkin.

Appellants argue that Chang does not teach, describe, or suggest "accessing transcodable content that comprises independently processable components to be encrypted, and encrypting at least one of said independently processable components". Appellant argues that Chang discloses that the processing of the component is dependent on associated metadata. Furthermore, appellant argues that the metadata is used to process a component, thereby introducing dependencies into the processing of the components. Applicant further argues that "the transcoding proxy receives the multiple messages corresponding to each component and inspects the metadata header of each message to determine which encrypted components should be selectively filtered".

As such, appellants understand that the transcoding of each component is dependent on the metadata for that component.

Examiner respectfully disagrees. Appellant's definition of "independently processable components" is as follows: "independently identifiable content components that can be independently (e.g. separately) encrypted/decrypted, encoded/decoded and authenticated". It is examiner's understanding of the current claim language that as long as the content components can be encrypted/decrypted independently, they can be considered independently processable components. In response to appellant's argument that Chang does not disclose independently processable components because Chang teaches that the metadata is used to process a component, Examiner believes this to be a moot point. The component portion and metadata header taught by Chang can be viewed a single component or two separate components. If they are viewed as one single component, Chang still teaches that both the header and the content can be encrypted - "...each part of the message, whether metadata header or component portion, to be independently and distinctly encrypted" (col. 10, lines 31-34). The mere fact that the metadata is used to determine which encrypted components should be selectively filtered is completely unrelated to whether or not the components are independently encrypted. Appellant appears to be arguing that determining which components to be selectively filtered is not considered "independently processable". But it is clear from appellant's definition that processing is intended to mean encrypting/decrypting. Appellant is arguing a moot point because, as far as the claim is concerned, determining which components to be selectively filtered is unrelated to encrypting/decrypting. Even if the metadata and the content are viewed as two separate components, the above arguments still apply - the metadata and the content components can still be independently encrypted. The components taught by Chang, while dependent on metadata for certain processing, is not dependent on the metadata for the processing claimed by appellant – encrypting/decrypting.

Appellant further argues that Chang recites that "clear-text metadata preferably provides a semantic understanding of the absolute or relative importance/priority of the components with respect to each other, thereby facilitating the transcoding process. By disclosing that the metadata includes information describing the relative relationship of components for transcoding, Appellants respectfully submit that Chang discloses that the components are not independently processable."

Examiner, again respectfully disagrees. While it is true that the metadata provides a semantic understanding of the importance/priority of the components, this is unrelated to the processing of the components with respect to encryption/decryption. As taught by Chang, the metadata is used to selectively filter the components (based on importance/priority) after encryption of the components have occurred. Encryption and decryption processes are still independent in relation to each individual component, as has been explained above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Daniel L. Hoang/

Examiner, Art Unit 2436

Conferees:

Nasser Moazzami

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Kim Vu

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435